DECTEC

DECTEC INTERNATIONAL INC.

PP 92-234

P.O. BOX 2275, 1962 MILLS ROAD, SIDNEY, BRITISH COLUMBIA, CANADA V8L 3S8
PHONE: (604) 655-4463   FAX: (604) 655-3906

October 8, 1991

Ms Donna Searcy
Secretary, Federal Communications Commission
1919 M Street
Washington, DC 20515

Dear Ms. Searcy,

This letter is presented in support of a filing submitted to the Commission by the Consumer Satellite Coalition on July 1, 1991. The document filed by the CSC requested a public hearing/inquiry on the monopolistic business practices of General Instrument Corporation and the distribution and sale to consumers by the General Instrument division of Forstmann Little Corporation of a defective descrambling product which is used by consumers and cable operators to unscramble programming delivered over satellite.

As a research and development firm which has spent the past three years developing a universal scrambling system designed to run multiple encryption and decryption processes through one single decoder, we submit that General Instrument has deceived the public, the governments of the United States and Canada, television programmers, hollywood producers, satellite and consumer electronic retailers, and the manufacturers of Integrated Receiver Descramblers in the sales and upgrade programs associated with its Videocipher II scrambling system,(exhibit A).

Through our work as a well-respected research and development company who has been the recipient of Canadian Federal grant monies, (exhibit B); and through our experiences as the only company attempting to compete with General Instrument for decoder sales in the present TVRO/Cable marketplace, (exhibit C) - we support the request of CSC for an inquiry into the behavior and practices of General Instrument who has a stranglehold on the current Direct-to-Home satellite industry and who has supported the pirating of subscription television services and who has been the primary beneficiary in the pirate marketplace, (exhibit D).

The filing submitted by CSC offers documented argument that General Instrument intentionally enabled and encouraged on-going compromise of its Videocipher II decoders in order to 1). sell more decoders, and 2). cause its own product to become obsolete. To lend more evidence to this fact, General Instrument Corporation shipped thousands of Videocipher II decoders into Canada for several years when none of the programmers using Videocipher were allowed to sell their services into Canada, (exhibit E). The only purpose for purchasing a VCII in Canada was to watch programming that was not and could not be paid for or authorized. By GI's own admission their exist over 400,000 pirated VCIIs in Canada, which represents 98% of the Canadian marketplace, (exhibit F). And while the VCII is prohibited exportation into Mexico, there are over 1 million pirate GI decoders in Mexico. And while one of GI's largest distributors was charged with and admitted to illegally exporting VCII units, GI maintains a close relationship with the company and continues to sell product which they know is being shipped outside of the U.S. and Canada.

Also, two years ago while we were involved in our own R&D program to develop a universal scrambling system, we contacted U.S. programmers to inform them that their Videocipher system could be secured. General Instrument, however, was not interested in securing the programmers' signals, (exhibit G).

Admitting now that the Videocipher II system has been pirated, GI expects to upgrade all cable systems and TVRO consumers to their new PLUS version of the same technology, (exhibit H). "When the PLUS is broken," says GI, consumers will be upgraded to a Renewable Security version which was announced to programmers shortly after GI illegally appropriated our own "smart card" technology. The RS version of Videocipher which has been reported by trade press as not yet in existence is also reported to contain a modem-on-module technology which will provide General Instrument with a slice of the revenues received by pay per view programmers.

Following RS, General Instrument expects to upgrade the entire cable and satellite market to its Digicipher system. Presently, General Instrument is tying the acceptance of Digicipher to the present chaos surrounding VCII, and they are putting a great deal of pressure on programmers to support and purchase Digicipher in advance. There is no reason to assume that should the Digicipher system be brought about as a de facto industry standard, that General Instrument would alter its present position on licensing and manufacturing. As was brought out by the CSC filing, "competition is limited by the fact that Channel Master (the only VCII manufacturer other than GI, yet who was appointed by GI) must purchase certain proprietary chips from GI." This type of fraudulent licensing and monopolistic control is likely to be perpetuated with Digicipher. It is the existence of this condition that enables our competitor to manipulate the industry for its own singular advantage.

We believe that if General Instrument were to conduct business in the face of true competition, the company would be more attentive to the needs of its customers and they would spend more time perfecting the technology of Digicipher in order to gain acceptance on the technical merits of the system rather than use complex contractual negotiations and threats to secure their position in the future high definition/compression market place.
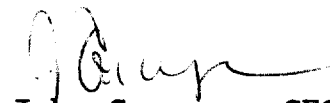
As a small company, we look to the free enterprise system as a framework through which ourselves or any other company is offered the opportunity to provide a better technology, a lower price, or more customer satisfaction. As the situation exists today whereby General Instrument is allowed the freedom to conduct business as an unregulated monopoly, the free enterprise system breaks down and the market place is not allowed to develop. However, even in the face of a major disinformation campaign launched by our competitor, (exhibit I), and despite the limitations of our own resources, our product competes against GI's VCII and VCII PLUS, (exhibit J).

Presently, we are shipping into Canada and are readying shipments into the U.S. of a universal decoder which is able to process VCII encrypted signals. Consumers are able to purchase either a VCII or a Secure Universal Norm decoder in order to pay for and be authorized to receive subscription programming. As all of the unit's parts are off-the-shelf and Made-in-America, any manufacturer of IRDs or consumer electronics is able to produce S.U.N. decoder modules, saving the industry over $40 million dollars while securing millions of dollars in programming revenue now lost to piracy.

It is the fact that the FCC in its inquiry into the satellite encryption marketplace has recognized Videocipher as the de facto industry standard that the satellite industry's trade association (SBCA) claims they must work with GI to cause consumers to purchase new GI product, (exhibit K).

We respectfully submit this letter of support and the attached material to request the Commission to consider scheduling a hearing/inquiry into the behavior of General Instrument. We look forward to competing on a level playing field with the rules of free enterprise properly in place.

Sincerely,

John Grayson, CEO
DECTEC International Inc.

Exhibits:

A: ON SAT, "GI Blues," December 2, 1990, by Bill Barr.

B: EE Times, "DECTEC Uplink Funded," January 7, 1991 by Richard Doherty

C.1: Times Colonist, "Local Firm Hitches Wagon to Satellite TV technology", September 8, 1991, by Jeff Bell.

C.2: Multichannel News, "GI and DECTEC Scramble Over Descramblers", September 16, 1991 by Gary Kim.

C.3: Signal Magazine, "S.U.N. is on the Horizon - What will we see when it shines?" June/July 1991 by Karen JP Howes.

C.4: Crosscurrents of Alberta Engineering Times, "DECTEC Challenges Videocipher," Winter 1990, by Larry Kelly.

D.1: Consumer Satellite Coalition, "Petition for Inquiry/Hearing, For Removal of GI Corp. Decoder Monopoly Status in Home Satellite Dish Marketplace", July 1, 1991 by Sue Baechler and consultant's name.

D.2: Intellectual Property Fraud Reporter,"DECTEC Accuses General Instrument of Piracy and Infringement in Canadian Law Suit", July 29, 1991, by Covington & Burling.

E.1: ONSAT, "Another ECM Wave", January 24, 1988, by Bill Barr.

E.2: ONSAT, "Chairman Alarms Dishheads," March 17, 1991, by Bill Barr.

F.1: EE Times, "GI tips pirate proof fix for Videocipher II," July 15, 1991, by Richard Doherty.

G.1: Copy of letter sent by DECTEC to Reiss Media programmer to provide information on stopping piracy, September 15, 1989.

H.1: TVRO Dealer, "Videocipher Upgrade/Conversion Update," (second in a series), October 1991, by David Hartshorn.

H.2: ONSAT, "Damned if you do - Damned if you don't," April 1, 1990, by Bill Barr.

H.3: Transponder, "The $64,000 Question,"August 1991, by Robyn Adair.

H.4: TVRO Dealer, "Videocipher Upgrade/Conversion Update," (first in a series), September 1991, by David Hartshorn.

I.1: Letter from Dectec attorneys, Jones and Emery, to GI, January 17, 1991.

I.2: Letter from DECTEC to Honorable P. Beatty of the Canadian Department of Communication, August, 28, 1991.

I.3: Letter from DECTEC to William Sessions, Director of the FBI, September 9, 1991.

J.1: TVRO Dealer, "DECTEC's On DECK", August 1991 , by David Hartsthorne.

K.1: Letter from Chuck Hewitt to Dectec and attached FCC notice, September 23, 1991.
K.2: Speech on S.U.N. System presented before the Subcommittee for Transitional Marketing of the SBCA, September 19, 1991.
K.3: Press release from GI, "General Instrument, SBCA Launch Program to Convert Owners of Illegally Modified Satellite TV Descramblers," May 1, 1989.

Exhibit A

What's Happening? by Bill Barr

G.I. BLUES

SAN DIEGO...Earlier this year, when the new, and supposedly secure, VideoCipher II Plus module was introduced, its manufacturer, General Instrument (G.I.), told the world they had ceased producing the old insecure VC II on the first week of June. The VideoCipher module fits into a drawer at the back of your integrated receiver/decoder (IRD) to unscramble VideoCipher scrambled programming.

This revelation created a buzz in the Canadian satellite industry and sent everyone wondering when the supply of old modules would dry up, thereby forcing anyone purchasing a new satellite system to pay for programming. Or, conversely, a break would occur on the new VC II Plus.

Distributors scrambled to purchase as many old VC II units as possible, at whatever price, as the price of old modules escalated dramatically. Distributors were ascribing to a proven theory based on past VideoCipher design changes; whoever has the most old modules hangs in the longest and makes the most money. It's a well known fact that in Canada 99.9% of the old VC II modules have been "tricked" and not paying for programming, the figure is 70% in the United States. This makes old VC II modules a very precious and sought after commodity.

Up to now, the security of the VC II Plus is holding. The "Rocket Scientists" told Onsat that it will be some time before the Plus is broken. Their perception is, an upgrade kit, allowing the old VC II modules to get the 200 VC II Plus upper channels, is more practical and easier to do. The present VC II decoders can only handle 56 channels whereas the Plus decodes 256.

As time passed, and the supply of old modules slowly diminished, General Instrument and Toshiba began shipping IRD receivers exclusively with Plus modules. This proved to be the "kiss of death" and their sales plummeted. The only way these brands sold was if the distributor, or dealer, swapped the Plus module for

the old insecure VC II that can then be chipped.

In October, just when the bottom-of-the-barrel of old VC II modules seemed to be approaching, an abundant supply of old modules began arriving in Canada marked "Remanufactured in Mexico". Some had manufacturing date codes of September 6. Others came from Channel Master, who produces VideoCipher modules for G.I. under license, with date stamps of June 16. So much for G.I.'s statement that production of old boards ceased June 7.

OnSat tracked these modules to G.I.'s repair facilities in Juarez, Mexico. As it turned out, they were VC II modules that were returned by the over 300 G.I. approved VideoCipher Module Service Dealer (VMSD) repair facilities. Nothing was scrapped. They were repaired in Mexico and returned to the marketplace. Programmers were astounded by this OnSat revelation.

Not only is this highly unethical, it proves beyond a doubt, that G.I.'s top priority is not signal security, it's making money, lots of money! .

G.I. argued that a customer wants a VC II module back in return for the defunct VC II he returns for repair. But OnSat has proven that customers never got a repaired VC II unit back, the VMSD installed a VC II Plus and sold the old modules to Canada, or elsewhere, for a $300 premium, plus a VC II Plus module. In fact, G.I. got $200 for some of the returned and recycled boards under their exchange for a VC II Plus scheme. By sending these back into the field, G.I. has the potential of getting another $200, if they are returned a second time, when people upgrade to the VC II Plus in search of popular programming, such as pay-per-view, who announced plans to migrate to the upper 56 tier bits next year.

Mike Meltzer, a spokesman for G.I., said he wasn't aware of this recycling practice. Either he is incredibly naive, or he is being dishonest, because Bob Caird of HBO and Rik Hawkins of the SBCA confirmed they asked G.I. six months ago to stop this practice and destroy the returned VC II units and replace them with a VC II Plus.

Now that OnSat has caught G.I. with its pants down on a cold Canadian winter's night, it remains to be seen if they will instigate ethical business practices and forsake their obvious hellbent quest for profit at the expense of their customers - the programmers using the VideoCipher scrambling system.

Several stories related to G.I's Mexican connection are still developing. One concerns U.S. Customs, who have spent millions to try and prevent VideoCipher decoders from being shipped to Mexico or the Caribbean in contravention of a State Department ban. This, because the VideoCipher sound decoding process uses a military secure algorithm called Digital Encryption Standard (DES). Anything using DES requires a munitions control export license. Canada is the only country waived from requiring this permit.

How can G.I. export product to their Juarez plant with DES in the U5 and U7 chips, when, just this past week, two executives of Recreational Sports, a large U.S. distributor, were fined $30,000 each after pleading guilty to illegally shipping VideoCipher decoders to Mexico? Another U.S. distributor, Starcom of Texas, was raided this week for the second time and the employees of their Mission branch were charged with similar practices.

I'm sure more of this G.I. dirty laundry will be fully aired in a future issue of What's Happening?

OnSat has also learned that four employees at the Juarez plant were fired recently for selling the precious VC II modules out the back door.

If you don't know what it's like to be caught with your pants down on a Canadian winter's night? Go outside and try it, not only is it embarrassing, it hurts real bad.

STARTED OVER

MISSISSAUGA...Only a year after being awarded the General Instrument (G.I.) product line for western Canada, Sherris Communications Inc. grew into one of G.I.'s largest distributors. This success has prompted G.I. to award Sherris Communications the G.I. satellite product line nationally.

Evan Sherris, owner of Sherris Communications, started Cale Communications in Regina, Saskatchewan in 1980, and in 1987 it was the second largest distributor of satellite products in Canada when it merged with Tee-Comm. A disagreement led Sherris to start over in 1989 with an outlet in Mississauga. He soon expanded back to Regina, and has never looked back.

Any component distributor knows that, with the right products, you can be very successful. G.I. makes good products! I'm sure this agreement will make Sherris into a leading force in the Canadian satellite industry, again! ◻

Exhibit B

Decoder uplink funded

BY RICHARD DOHERTY

Sidney, British Columbia — DEC-TEC International last week received a boost in its effort to build the industry's first reprogrammable satellite head-end uplink, when it was awarded a cash grant by the National Research Council of Canada.

While General Instrument Corp. was announcing that it will be ready to repel boarders within a year (see related story, this page), DECTEC is preparing, with the help of the grant, to complete its uplink here by March 31. DECTEC then will demonstrate to the Canadian government and others how its Secure Universal Norm (SUN) video-decryption architecture "makes piracy virtually impossible," according to DECTEC president John Grayson.

DECTEC's grant announcement came only days after GI said it is resorting to a field-replaceable "smart card" of its own design if piracy problems arise with its VideoCipher II Plus descrambling system.

DECTEC plans to use the programmable satellite-uplink facility to demonstrate an ability to simultaneously address multiple video-encryption systems from one site. Such a demonstration would help the company generate commercial interest in the programmable gate array-based SUN architecture (see Oct. 22, page 1)

Private channels

"In a SUN environment, each channel behaves like a private network, with a private scrambling system. In other words, if one programmer or broadcaster is compromised, all of the others remain secure," Grayson said. Because SUN does not allow for common, or shared, "keys," there is little chance of piracy of multiple programs," said Grayson.

In contrast, GI has always placed its programmer customers on "tiers" of digital encryption. So, when techno-pirates had scaled one digital defense wall, they were awarded with several program choices at one time.

Last fall, DECTEC tapped Xilinx Inc.'s programmable gate-array technology and Dallas Semiconductor's static RAM modules to demonstrate a single satellite-receiver module that can decrypt more than one video format at a time. Since then, DECTEC decided to create its own uplink site, because it lacked official access to the most popular data stream uplink, GI's VideoCipher system.

DECTEC is trying to challenge GI's dominance of the 2 million satellite-decryption-module market. GI uplinks VideoCipher II and VideoCipher II Plus entertainment and sports to 3 million North American dish owners and to the cable TV head-ends that supply most of American cable-TV programming.

But GI's problems in ensuring adequate data security for its system have prompted programmers to evaluate rival technologies. Because SUN can emulate multiple satellite-decryption schemes, it has the potential to minimize the electronic-cabling clutter that would occur if multiple satellite-decryption boxes are needed for each household that has a dish.

Meanwhile, a spate of higher-power C and Ku-band satellites are expected to be launched this year and next,

---

Because SUN does not allow for common, or shared, 'keys,' there is little chance of piracy of multiple programs, said DecTec president John Grayson.

---

creating new markets for smaller dish systems. So, programmers are eager to serve the additional dish audience with secure and convenient subscription programming.

DECTEC performed a blind engineering of the VideoCipher II data stream by monitoring it from space at its teleport center here. As a result, DECTEC, and many industry engineers, believe SUN does not infringe on any GI patents or computer-code copyrights. (Similar precedents exist in the computer industry for blind-engineered systems.)

The grant represents 20 percent of DECTEC's 1991 R&D budget and is the second one awarded to the Canadian company. The grant was made under the NRC's Industrial Research Assistance Program, an analog to the American Small Business Industrial Research grant program.

Exhibit C

BUSINESS

MAGAZINE

Local firm hitches wagon to satellite TV technology

By Jeff Bell

An acronym may be raising acrimony with the competition, but the future looks bright for a Sidney electronics firm that has developed a television scrambling system decoder dubbed the SUN.

DECTEC International is sure its fortunes will rise considerably when the SUN — or Secure Universal Norm — secures its place in the burgeoning satellite-television market.

The SUN system hit the Canadian market in force Aug. 1. Its production will be handled by distributors across the country.

The system performed well during six months of field tests at 3,500 sites across Canada earlier this year, giving DECTEC president John Grayson cause for optimism that the SUN decoder will make an impact in a Canadian market where satellite reception is the only means of access to television for over two million homes. Distributors had already placed orders in the thousands early this year long before the SUN was scheduled for sale.

It was a definite sign, Grayson said in a January news release, that "we're going to be growing very big very quickly.

"And we know we have to stay focused, be cautious and somehow still have fun."

Grayson was further buoyed by an enthusiastic reception from American cable programmers in July meetings in New York. He is also considering DECTEC's prospects in the European market after presenting a paper on the SUN in May at the MediaVille '91 conference in France

and speaking at the invitation of Canada's Department of External Affairs and International Trade at the 17th International Television and Technical Exhibition in Switzerland.

Because some of the existing technology in Europe has a basis similar to the SUN, marketing it there would be "a different kettle of fish" than in North America, Grayson says.

"There may be some opportunities in Europe, but we will concentrate our efforts on North America first. The real opportunity as I see it is the global marketplace — there is a potential market of nearly a billion units now, and new cable systems ready to go in places like Zaire."

Grayson predicts that DECTEC's share of a market that is currently almost exclusively the domain of American-based General Instrument Corporation will be about 20 per cent within a year. That means production of almost 20,000 units a month, and DECTEC has already added two more staff — a business development officer and a systems expert — to help with the task.

The additions bring DECTEC's payroll to 23.

The importance of communications in today's world is virtual assurance of a strong market for products like the SUN that fill a need in satellite technology, Grayson says.

"Your options now are to be near a CBC repeater station or get a satellite dish and join the 20th century."

At present, most of the existing two-million satellite-decryption units serving the millions of
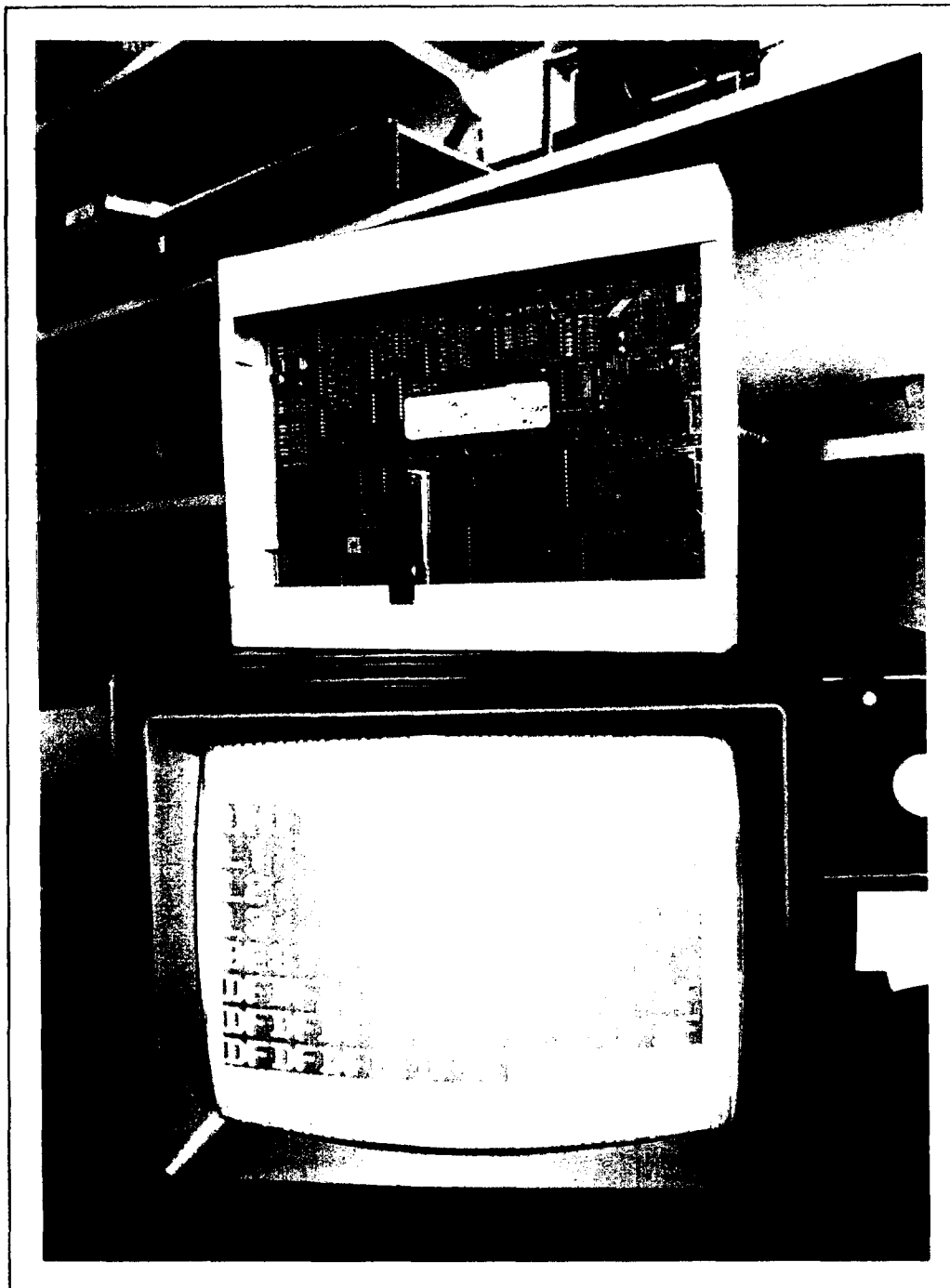
Computer chips made to descramble signals

satellite dish owners in North America are produced by GI, which is currently embroiled in a legal battle with DECTEC for what it sees as an infringement of its patent.

Court action by GI began June 3 in Toronto, and the company was unsuccessful in having DECTEC banned from producing the SUN while the case is in litigation.

"We've taken the high end and asked them to prove what they are saying about us, and responded with a $20 million damage suit against them," Grayson says.

As for GI's allegations, Grayson says they are baseless, a contention backed up by independent reports from Tredennick Inc., a prestigious U.S. engineering company, and the patent-law firm Seed and Berry.

The SUN merely emulates the function of GI's VideoCipher and other scrambling devices with its application of "smart card" technology, Grayson says. "We are essentially making software out of hardware with the smart card."

The "smart card" is a credit-card sized piece of plastic containing a micro-computer chip that inserts into the SUN decoder. "It contains a software description of what used to be a hardware device, and can do away with the need for replacing hardware as technology changes."

Smart-card technology greatly enhances programmability and security of scrambling systems, Grayson says.

But there is more than the superior function of the SUN system, which was three years and over $2.5 million in development, to throw a curve at the competition. Grayson says that Bill C-40, the new federal broadcast act passed in June, may lead to ban of products like the VideoCipher "or any similar device that can be used to intercept signals" without paying.

"It's hard to sell a program like ours when people can sell the public something like that."

"Pirating" of signals is costing programmers hundreds of millions of dollars annually, but a device like the SUN, which provides a secure and virtually unpirateable signal scrambling system, can mean an instant source of revenue for the companies involved, Grayson says.

"A secure scrambling system can allow the companies to protect their investments. There are estimates of considerable revenue for companies by getting rid of pirate boxes and using our system."
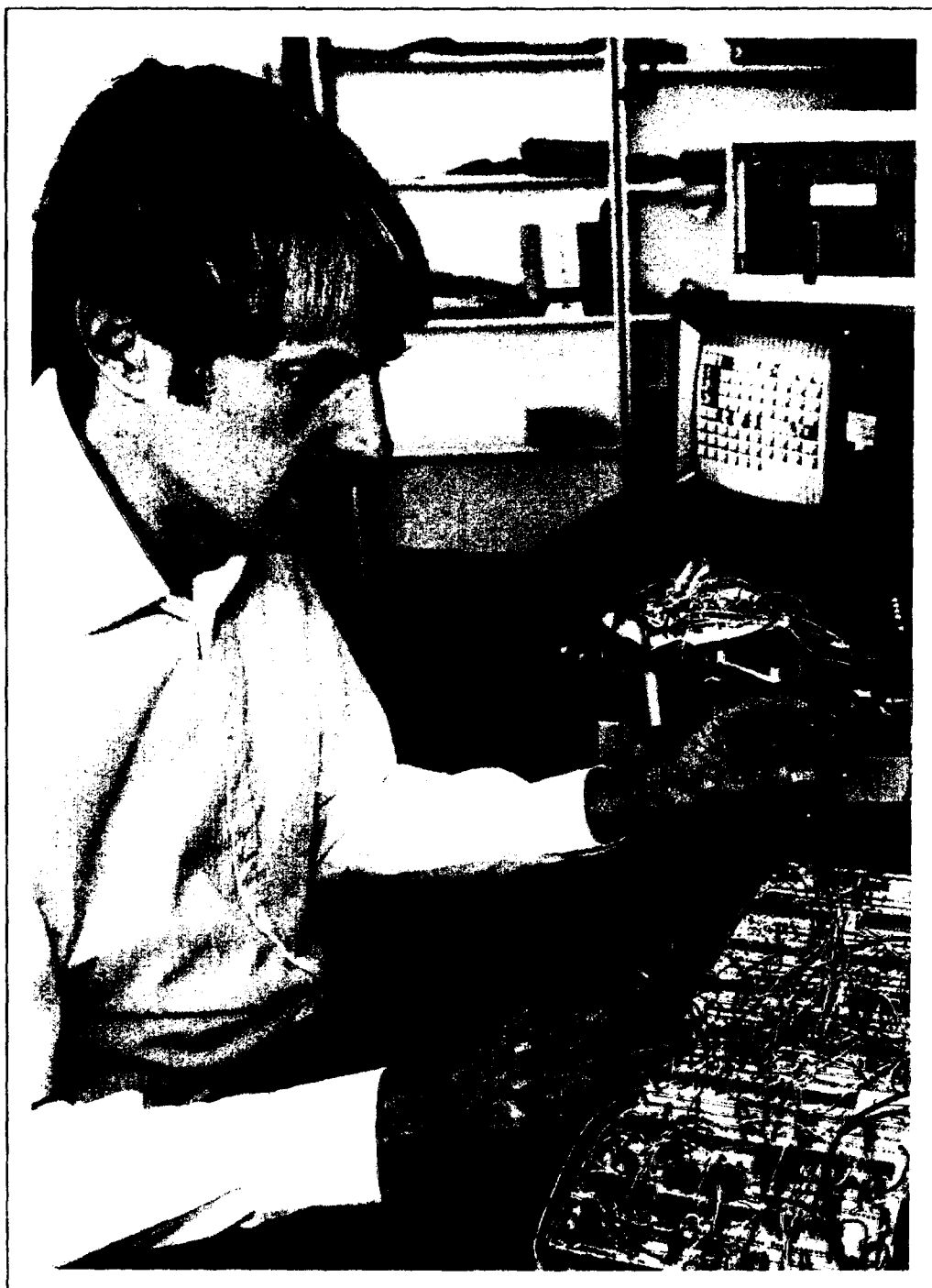
The independent estimates suggest for example, that Net-Link will realize an additional $15.84 million in an 18 month period and Arts and Enter-

Dectec employee works on satellite decryption project

tainment $2.28 million.

The SUN descrambler, a small unit about half the size of a computer keyboard, is essentially "a blank piece of digital canvas", Grayson explains.

"The SUN is not made using conventional chips, which are made to do only one thing, but with logic cell arrays." They are what give it such versatility, Grayson says.

Legal challenge or no, Grayson says the course is set for the SUN system to make an immediate impact in the satellite-communications industry in Canada. Positive assessments of the company's prospects go beyond its own doors, with the Electronic Industry Association of Alberta, for example, calling it "a company to watch in the '90s."

DECTEC

DECTEC INTERNATIONAL INC.
P.O. Box 2275, 1962 Mills Road
Sidney, British Columbia
V8L 3S8, Canada
Tel: (604) 655-4463
Fax: (604) 655-3865

Multichannel News

Multichannel News, the cable industry's leading newspaper providing up-to-the-minute information has a circulation of 15,000 and is distributed in countries throughout the world. 31

TECHNOLOGY

GI and Dectec Scramble Over Descramblers

By GARY KIM

One of the messiest technology patent battles ever to erupt in the cable TV industry appears poised to spew forth.

The protagonists: General Instrument Corp.'s VideoCipher division and DECTEC International Inc. of Sidney, British Columbia, which says it has begun shipping satellite descramblers that emulate the operation of Video-Cipher units without infringing on any protected technology GI owns.

DECTEC officials paint themselves as David to GI's Goliath and say their system is technically superior to GI's without using any proprietary technology.

GI, which appears to have been preparing a meticulous legal stratagem, hints that DECTEC is essentially a front for piracy, and assails DECTEC's claim to a more secure and flexible technology.

"We've already shown that his security system can be beaten," said GI legal counsel Ken Boschwitz.

VideoCipher officials say they intend to respond with further legal action "very soon," based on a standing injunction that bars ship-

> **Each side accuses the other of aiding and abetting signal piracy.**

ping of any DECTEC systems to customers in the United States or Canada, said VideoCipher spokesman Mike Meltzer.

DECTEC president John Grayson has countersued GI, charging that the design of the new VideoCipher "Renewable Security" sys-

tem itself is an infringement of DECTEC's "smart card" system.

Grayson argues that GI knows full well that he hasn't violated any patents because VideoCipher raided his offices and carted off software and system documentation.

In the fog of this war, each side accuses the other of aiding and abetting signal piracy. Grayson argues that all 400,000 VCII units in Canada are "compromised" and that GI knows it. Grayson says GI is shipping reconditioned VCII boxes into Canada that will only make the problem worse.

GI officials clearly believe Grayson has demonstrated ties to the "hacker" (computer enthusiast) community that is the chief source of VCII piracy.

Boschwitz suggested that DECTEC has the burden of proof since so far as he

knows, no programmers have agreements in place with DECTEC that would allow a claim that the boxes are intended only for legitimate, paying customers.

Expecting continued and expensive legal wrangling with GI, Grayson has amassed a $1 million "legal insurance fund."

The controversial Secure Universal Norm (SUN) descramblers DECTEC said it is shipping are said to be compatible with General Instrument Corp.'s VCII-Plus units (as well as with Oak Communications Orion descramblers) while offering a far more flexible and secure option at lower cost.

Several cable programmers, meanwhile, appear to have had discussions with DECTEC about the technology.

At least one leading programmer's engineering

director appears to have suggested that DECTEC build a cable TV headend version of its descrambler, aiming at the "hot standby" market.

Because the DECTEC units are designed for immediate reconfiguration by simple downloadable software changes, it's possible that they could be used to provide nearly instant backup for any VideoCipher descrambler circuit, Grayson said.

Providing that the operator has valid contracts in place, all that is required to make the switch is keying in the serial number of the defunct descrambler into the DECTEC unit, which then assumes the personality of the downed box, he said.

Grayson said a DECTEC unit costs about $395 against $795 for a comparable VCII.

S.U.N. Is On The Horizon - What Will We See When It Shines?

by Karen JP Howes

Last fall, DECTEC International Inc. completed the design of a satellite scrambling system called the Secure Universal Norm (S.U.N.). The system makers claim it will provide the satellite industry with a highly secure and functionally unpiratable signal scrambling system, and they say it doesn't require dealers, TVRO owners or

The S.U.N. descrambler is enclosed in a white plastic case bearing its name on a gold emblem at top centre. The descrambler itself contains no descrambling processes. The S.U.N. unit receives its instructions from a "Super Smart Card" which is plugged into the slot at the front of the S.U.N. unit. Security information is hidden deep within the self encrypting processor carried in the "Super Smart Card"

factured by General Instrument Corporation for the North American home satellite market, function as pirate devices. Programmers have lost hundreds of millions of dollars in revenue and the growth of the Direct-To-Home (DTH) business has been stymied.
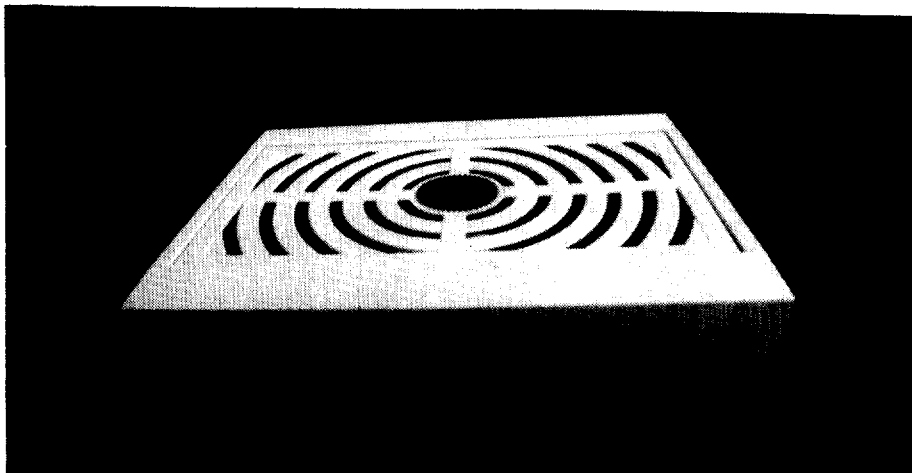
Two years ago, HBO and ESPN went so far as to form a joint venture to seek a new encryption system to replace Videocipher II and today most program-

sal, open architecture scrambling system shocked even the most openminded and drew pointed criticism from the skeptical.

In a letter drafted by Taylor Howard, head of research and development for Chaparral and technical consultant to the SBCA's anti-piracy task force, the author insightfully noted that "it (the S.U.N. decoder) is a well done piece of printed circuit board work that used field programmable gate arrays (FPGA) technology to emulate the, up till now, proprietary chips which GI has used to control the patent and copyright technology."

"Emulate," Mr. Howard continues, "is an important word here because much heat will be generated over the possibility of emulating without infringing."

Still, the general consensus remained that DECTEC's technological breakthrough was not really possible. So if it wasn't possible, it must be a deceptive trick. That explanation satisfied many. But the question arose, how much can any of us really know of what is possible in a constantly evolving and changing world comprised of things too small to touch, let alone see and truly comprehend.

programmers to change anything that is already in place.

But can a small Canadian R & D firm change the way we have been taught to understand satellite scrambling?

An Acquaintance With Scrambling

Within the past six years, each of us to one degree or another has become pseudo crypto-ites. We casually toss around neat new words once only familiar to cryptologists and mathematicians. Ask anyone else to word associate with "movie" and they'll say "popcorn". But from our psyche comes quirky nomenclature like seed keys, algorithm, sync inversion and DES.

Still most of us actually know very little about encryption. We expect it to be like our television. Turn it on and it works. But the technology hasn't been so gracious. Industry trade reports over the years have shown that anywhere from two to three million of the 3.2 million Videocipher descramblers, manu-

mers either believe that GI's PLUS version or its upcoming RS module will provide a secure solution, or they have thrown up their hands in disgust and have decided to await digital compression.

The New Kid Moves In

But last November, a small Canadian research and development firm unveiled a revolutionary approach to satellite scrambling. The company's claim that they had developed a univer-

Smart Cards

Since before Sony developed Telefirst for ABC, scrambling systems have been designed as closed architecture networks. Their design requires the system's functions to be hard wired into custom chips that are soldered into permanent board positions. This proprietary approach to product design functions such that when an encryption system provider sells his system to a user, the provider becomes the sole supplier of decoders and encoders for
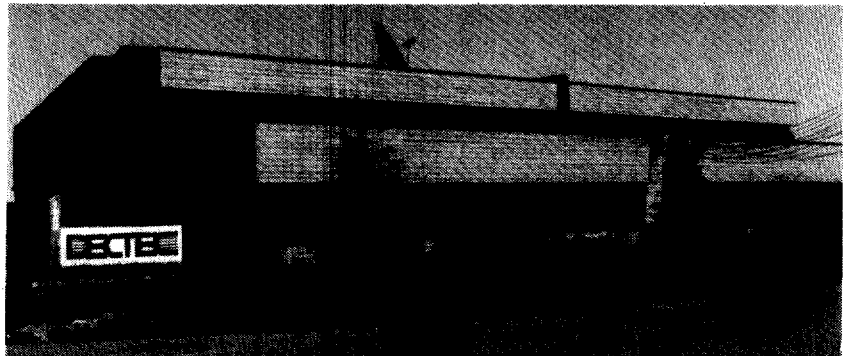
DECTEC's Offices in Sidney, British Columbia

the life of the network. If the system is compromised, security can be restored only by replacing each subscriber's decoder. Also, if the network owner decides to upgrade or alter features within his own system - e.g. the number of "tiers" - he must again undergo a system-wide replacement.

Because systems are hard wired and difficult to upgrade or replace, the commercial encryption industry has not been motivated to keep encryption technology up-to-date. In fact, even the most recently announced systems: Videocipher II Plus, Prime Star's version of BMAC and the updated Leitch, are still based on the technology of their parents and are conventional and closed by design. Some of these systems have been updated though as they will soon employ a smart card in order to keep the decryption key out of the actual descrambler. While the smart card approach, originated in North America by DECTEC, allows the system operator to replace smart cards when the security portion of the system is compromised, the functions and features provided by each of the "new" conventional systems are inherently unyielding.

An open architecture approach is more elegant. It leaves nothing of consequence within the decoder itself. All processes, algorithms, functions and features of the system are provided through software. The software tells the decoder how to behave. Thus, the same decoder box can be programmed to decrypt several different encryption processes.

Specifically, the first release of the S.U.N. system comes equipped with enough memory to simultaneously process two or three different descrambling programs. For example, one program designed to configure the S.U.N. decoder to behave as a Videocipher II unit can run concurrently with a second program providing S.U.N. with the characteristics to act like an Oak box. The S.U.N. box is designed to identify the scrambled signals coming into the box and automatically switch between the software programs loaded within.

Once the S.U.N. box is configured in any specific way, the unit's owner can only access a scrambled signal if he subscribes to, pays for and is authorized to be turned on. Where the S.U.N. system again differs from the conventional design is that the authorization process is reconfigurable. In the current VCII environment, S.U.N. units loaded with the appropriate software could be authorized through one of several methods including: through G.I.'s own DBS authorization center;

directly by the programmer through DECTEC's Universal Data Teleport or by way of a telephone line; or through smart card updates. (The latter works best for authorizing one time events distributed to a manageable number of receive sites).

Most surprising about the approach taken by DECTEC is that while DES systems like Videocipher require the same secret key to be used to both encrypt and decrypt data, S.U.N. is able to emulate the VCII system and provide authorization without the use of any of GI's seed keys.

John Grayson, CEO of DECTEC International Inc., explains that the Secure Universal Norm scrambling system is as different to conventional scrambling systems (like VCII, Oak, BMAC and Leitch) as algebra is different from geometry. While both are mathematics and either can be used to solve relational problems, the two are inherently different.

The Dawn of SUN

DECTEC first departed from the conventional approach to scrambling three years ago during a preliminary planning session. "We were focused from day one", explains Mr. Grayson. "We weren't interested in offering just another scrambling system. We knew DBS was on its way and we understood what the DTH industry was going through. We wanted to develop a technology that would make it possible for the consumer to have one decoder in his home yet leave open the method and application of encryption and authentication on an ongoing basis".

So, sketched on a piece of company letterhead dusted by sand and cool Canadian sea air, Grayson wrote these notes: 1.) compatible with Videocipher and Oak; capable of being configured to offer BMAC, 2.) functionally unbreakable and 3.) changeable.

A nice idea. But it didn't seem possible. That is, until one year later when a company out of San Jose unveiled new developments in gate array technology. Fascinating breakthroughs in field programmable gate arrays and, specifically, Logic Cell Arrays, brought Grayson back to his salt-washed notes. He then teamed up with a notable British scientist and began the arduous process of research and development which not only involved the blind-engineering of the Videocipher technology but also required DECTEC's engineers to push the design parameters of FPGAs.

Meanwhile, back in the civilized world we were becoming more and more acquainted with conventional scrambling.

John Grayson, CEO DECTEC International

We were taught about encryption methods, the difference between hard and soft scrambling. We rehearsed which keys did what and we were beginning to get the gist of what it all meant. But still at the forefront was the damage created by piracy.

Night Falls On Firmware

Essentially, scrambling eludes us because its physical presence is beyond our perception. The processes, features and functions of scrambling systems are based on mathematics. This is why DECTEC engineers were able to tap into the power of reprogrammable gate arrays to create the first universal scrambling system and enable what was once done in firmware to be provided through software.

While this open architecture approach is dramatically different from what we have become acquainted with over the past six years, if it proves to offer greater security and more system flexibility - if it can allow several encryption systems to be processed through one piece of consumer hardware, and if it can offer choice and competition where none has previously been allowed to exist, then maybe some of us can forego yet another learning process and know simply that, when we turn it on, it will work, and that we won't have a pile of different decoder boxes stacked on top of our TVs.

In Summary

DECTEC's technological breakthrough was fundamentally designed to provide consumer, programmer and present or future scrambling makers with a universal platform through which competition and innovation would flourish.

"We realize that our S.U.N. system disrupts the status quo," explains Mr. Grayson, "so we plan to bring the Secure Universal Norm scrambling system to the DTH market as we brought its design from drawing board to finished product. We will proceed in an orderly and focused manner."

The Fundamentals of Signal Scrambling and How They Relate to S.U.N.
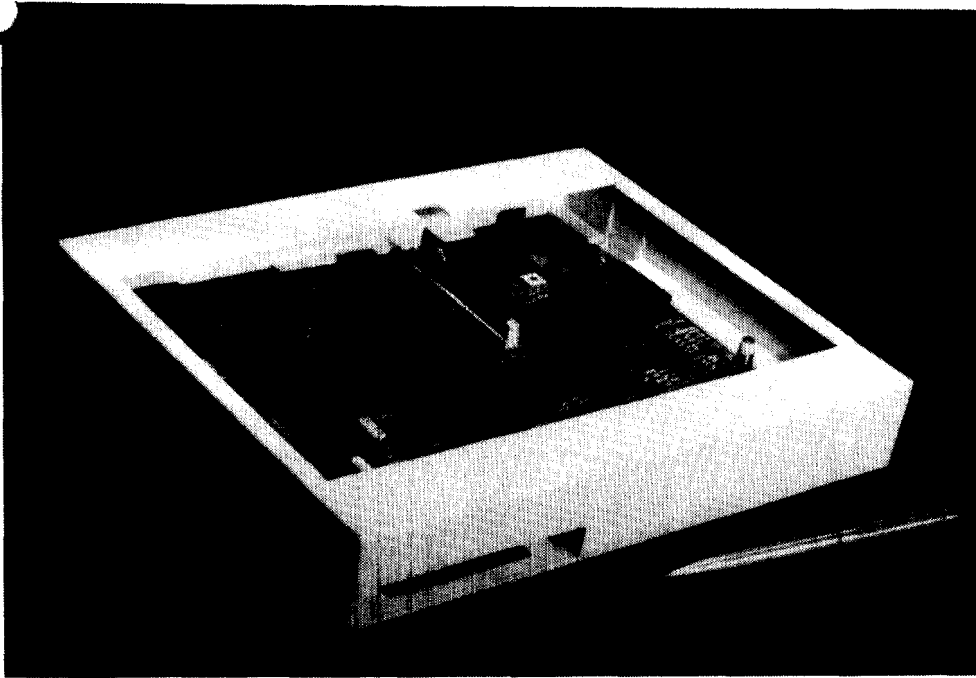
The Locks

Signal scrambling can be divided into two areas of discussion - 1. the method of scrambling/descrambling and encrypting/decrypting signals and 2. the method of managing, securing and communicating the information which enables the first step to occur.

In the past we focused our attention on the first area, how to attain the most secure scrambling/descrambling procedure at the least cost. Initial experience showed us that some analog scrambling techniques were simple and inexpensive to crack.

Patrice Peyret, product development manager at *Gemplus Card International* Inc., says that most analog scrambling systems involving RF-level scrambling and sync modification are relatively insecure since any person with knowledge of frequency characteristics and equipped with receivers outfitted with sophisticated sync separation circuitry can easily display an undistributed picture.

Oak Orion, for example, employs a video scrambling method which randomly alternates between various inversion modes. In the Videocipher II system, video information is inverted between sync pulses and then suppressed. According to Tom Shimabukoro, Director of systems planning and analysis for GTE's Spacenet and author of Securing the Corporate Vil-

lage, Oak's video scrambling technique is more secure than VCII's.

Analog scrambling systems based on modifying the active part of the video signal, states Peyret, are more secure. The Line Cut and Rotate method used by both Videocrypt and Eurocrypt, and the popular Video Line Shuffling process used by Leitch both require the use of real time spectrum analysis to reverse the distorted condition. But the most secure form of scrambling, per se, is when a signal is processed digitally, sampled, then randomly intermixed.

The audio portions of VCII, Oak and BMAC and both video and audio signals within the Leitch commercial unit and VCI are hard scrambled - that is, the analog signal is converted into binary streams comprised of zeros and ones. Once digitized, the signal's sequence is mathematically manipulated (for example, run through a complicated algorithm like DES or any other polynomial). Conversion back to the analog format produces a distorted signal unless a decoder is given the key to reverse the original equation. This is why many now look forward to the sterile digitized environment of compression where we believe that the security of a digital system is based on how "difficult" is the mathematical formula creating the cryptosystem.

It's the same premise that led VCII designers to first claim their system was unbreakable. And they were right if they considered the entire system to be the process of encrypting the audio signal through the DES algorithm.

Theoretically, the only way to break DES is to try every possible key to find which one transforms ciphered text into
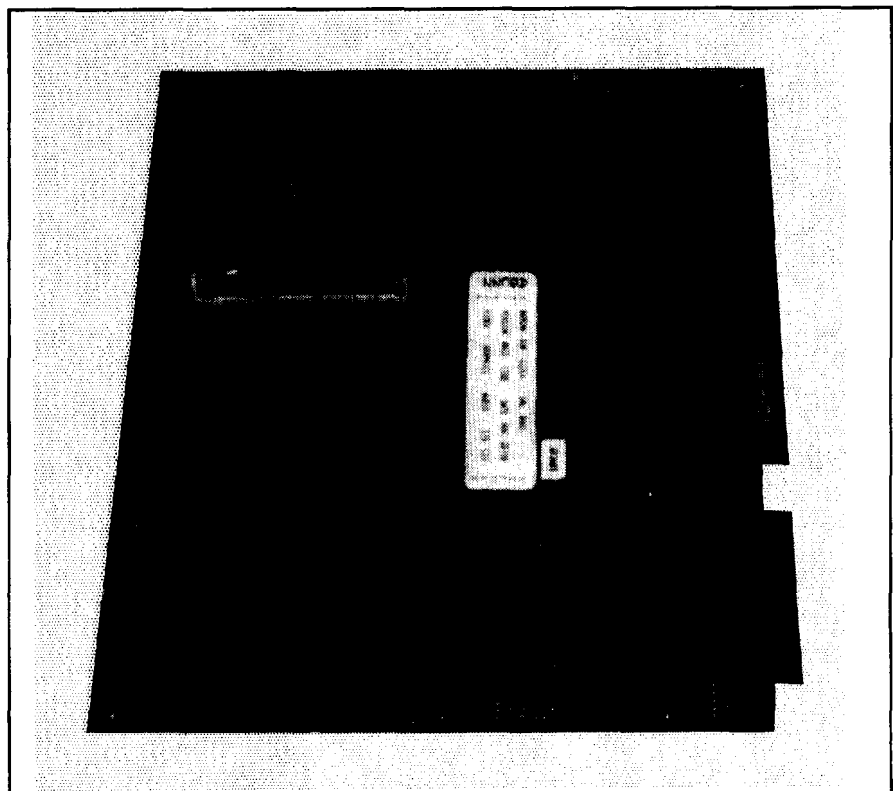
recognizable information. In the DES process, each key is 56 bits long, creating some 72 quadrillion possible keys. Even in using a high speed computer capable of running 10,000 DES operations per second, it would take 114,246 years to find 1 key. But who needs to sit at a computer for 100 centuries if the decryption key is accessible? The best lock (or algorithm) won't keep out trespasser if the key is always kept under the door mat. This realization is what has most recently turned our attention to the second area - the key management aspect of scrambling.

The Keys

According to James Bidzos, president RSA Security," . . . the greatest weakness in any cryptosystem is the handling of keys." Insecure management of keys and access control systems is what enabled hackers to break Oak, VCII, and BMAC. It is also why PLUS is expected to be broken and why even digital compression is vulnerable to breaches in security. We now have at our disposal a host of reasonably unsolvable algorithms which have given us a secure lock. So we now move on to consider how we can best transport and store the key that opens the lock.

In the conventional approach, a handshake is required whereby the sender provides the receiver with a common key which is used to both encrypt and decrypt data. The common key is combined with another key which is embedded into the physical decoder. The fact that a key is put in one place is what makes a system penetrable.

The S.U.N. system, however, does not require a handshake and the control data is neither stationary nor accessible.

Through DECTEC's open architecture approach, the keys - which are replaceable and carried on a removable smart card - are themselves encrypted with a complex mathematical algorithm. It is the same system employed in Europe for electronic bank transfers. But the very nature of the logic-based, universal platform developed by DECTEC has provided the Secure Universal Norm with an additional and perhaps more deterring safeguard. Within S.U.N. not only can the keys be continually and randomly repositioned and replaced, but the lock can also be changed.

Because S.U.N. can be completely reconfigured in the field at any time, the entire digital processing scheme can be changed. Where both the keys and locks can be easily and cost effectively altered, the system becomes functionally unbreakable.
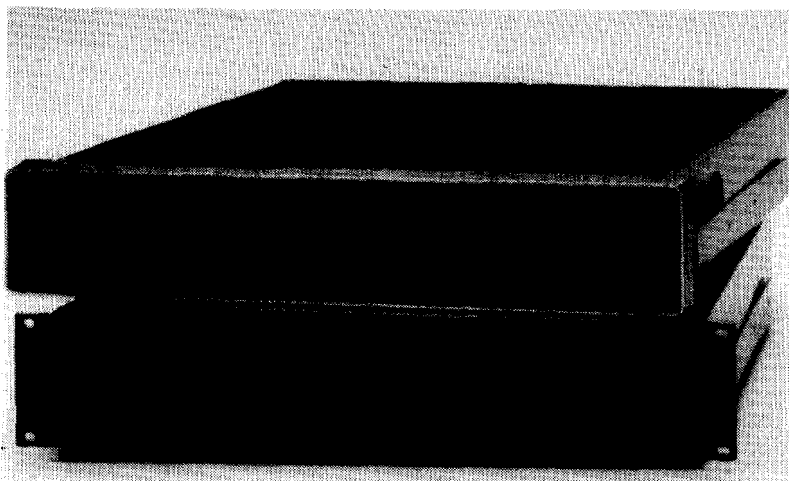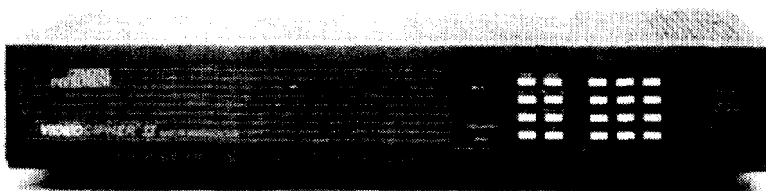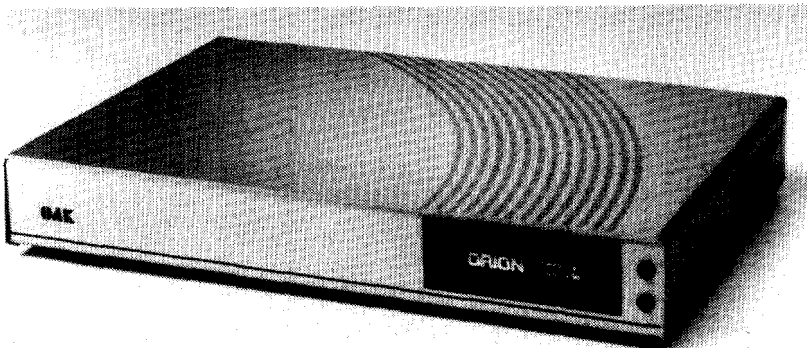

A sampling of existing descrambling products;
Top: Oak Orion - Middle: General Instrument VideoCipher II - Bottom: Leitch ViewGuard

DECTEC International Inc.

P.O. Box 2275

1962 Mills Road,

Sidney, British Columbia,

Canada V8L 3S8

Phone: (604) 655-4463

WINTER 1990

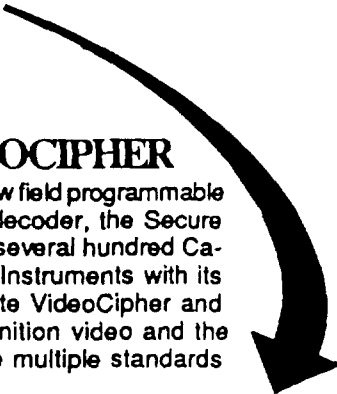## CANADIAN FIRM CHALLENGES VIDEOCIPHER

DecTec International Inc., of Sidney, B.C., has used Xilinx's new field programmable logic chips to create the world's first reconfigurable video decoder, the Secure Universal Norm (SUN). The product, which is in beta test at several hundred Canadian sites, removes a virtual monopoly held by General Instruments with its VideoCipher II technology. The DecTec product can emulate VideoCipher and Orion decoders and will be able to handle enhanced definition video and the proposed digital encryption standards. It can even manage multiple standards in case users have both dishes and cable.

The basis of the product are six Xilinx RAM based logic blocks. These chips use static RAM to hold the programming data instead of EPROM cells or fuses. When the system is powered up, configuration information is downloaded into the Xilinx CMOS chips which then create the required circuitry. A new configuration can even be downloaded via satellite. It takes about a second to change from one encryption standard to the next.

> *DecTec's technology will position it to command a large chunk of the future market.*

General Instruments, which acquired the VideoCipher II technology from M/A-Com Linkabit three years ago, may not let this intrusion go unchallenged. G.I. is considering legal action to protect what has become a billion dollar plus industry for them. DecTec claims it has reviewed the GI patents and studiously avoided any infringement. G.I. claims that DecTec's technology will open the door to signal piracy. However, the VideoCipher boxes are known for allowing an already outrageous amount of piracy. About 2 million VC II boxes have been sold but there were less than 700,000 authorized users as of September '90. There is even a Caribbean 900 number which VC II owners can call to obtain the current month's program authorization keys. DecTec's flexible architecture represents a moving target for pirates and will be able to provide advanced security features as they are developed.

DecTec's technology has a number of features which will position it to command a large chunk of the future decoder market: It can host multiple emulations at one time, it is field programmable, it uses off-the-shelf components which aids repair and it can handle large bandwidth video signals. This is indeed a company to watch in the '90s.

Exhibit D

TO THE

F E D E R A L   C O M M U N I C A T I O N S   C O M M I S S I O N

WASHINGTON, DC   20554

In the Matter of

Petition For Inquiry/Hearing Under First
Amendment Rights Of The People To Petition
The Government For A Redress Of Grievances
By Consumers and Other Interested Parties
Against General Instruments Corporation's
Monopolistic Decoder Business Practices
And Removal Thereof.

TO: The Commission

PETITION FOR INQUIRY/HEARING

For Removal Of General Instrument
Corporation's Decoder Monopoly Status
In Home Satellite Dish Marketplace

CONSUMER SATELLITE
COALITION
Route 4, Box 169
Macon, MO   63552
(816) 385-2526

Technical Consultant:

Allan E. Stahl, Consulting Engineer
8 Cedar Street
St. Albans, VT   05478
(802) 524-5637

July 1, 1991

INTRODUCTION

The Consumer Satellite Coalition (CSC) is a national grass root organization that officially represents over 2,176,000 Home Satellite Dish consumers who are the customers of the Satellite Dealer Coalition (SDC) dealer members and others.

In all the FCC decision making since 1986, concerning General Instruments Corporation as the monopoly decoder manufacture, the FCC has not held hearings for the TVRO consumers and other interested parties who use the General Instruments products and who are affected by the use of said products.

This petition is a request for a public hearing/inquiry by the FCC under the peoples First Amendment Rights to petition the Government for a redress of grievances, to show just cause as to why General Instruments Corporation should no longer be granted a government sanctioned monopoly status in the TVRO industry marketplace.

Consumer comments, questions and documented testimonies, articles and consumer signed petitions are enclosed in this petition for your review, to help you to expeditiously set a date for the hearing/inquiry with participation from consumer witnesses and other interested parties.

General Instruments Corporation has played a central role in the VideoCipher encryption mess for the last five years. Should it be allowed to continue profiting from its de facto monopoly by granting it a governmentally-decreed monopoly? We think it is time to let a free marketplace operate freely.

TABLE OF CONTENTS

APPENDIX

TVRO CONSUMER SIGNED PETITIONS

SUMMARY

TVRO CONSUMERS FEEL THE TVRO INDUSTRY COULD BE SUMMED UP BY ONE WORD:
<u>MONOPOLY</u>:

The **Consumer Satellite Coalition** chooses to use the words of James E. Scott, Editor for TVRO Dealer, which best describes what is going on in the TVRO industry:

Freedom of choice is why this country was begun, and what it represents to the rest of the world. But this industry has very little freedom of choice. Once you get away from the dish, feedhorn, LNB and mount, there's hardly anything else in TVRO that's not directly impacted by the de facto encryption monopoly that the VideoCipher represents:

* Look at the incredible waste of time and money (not to mention exquisite agony) it's taking to try to get dozens of programmers together long enough to do something as simple as halt piracy by turning off the VCII datastream.

* Precious monies that should be spent by it's trade association to promote and develop the TVRO industry are spent to defeat piracy caused by the monopoly encryption datastream.

* This monopoly not only helped create piracy but also has aided and abetted its sustained growth for the last five (5) years.

* Receiver manufactures must have their new designs approved by a competitor, which also is the owner of the monopoly encryption device vendor.

* Programmers have only one choice when it comes to authorizing their customers: through the "Non-profit" DBS center owned by the monopoly encryption device vendor.

* In a competitive electronics environment, prices always drop as the market matures. In TVRO, because of the monopoly, they keep going up.

* Monies from the monopoly encryption device vendor help keep the main trade association afloat and helped this main trade association buy ownership of it's own trade shows.